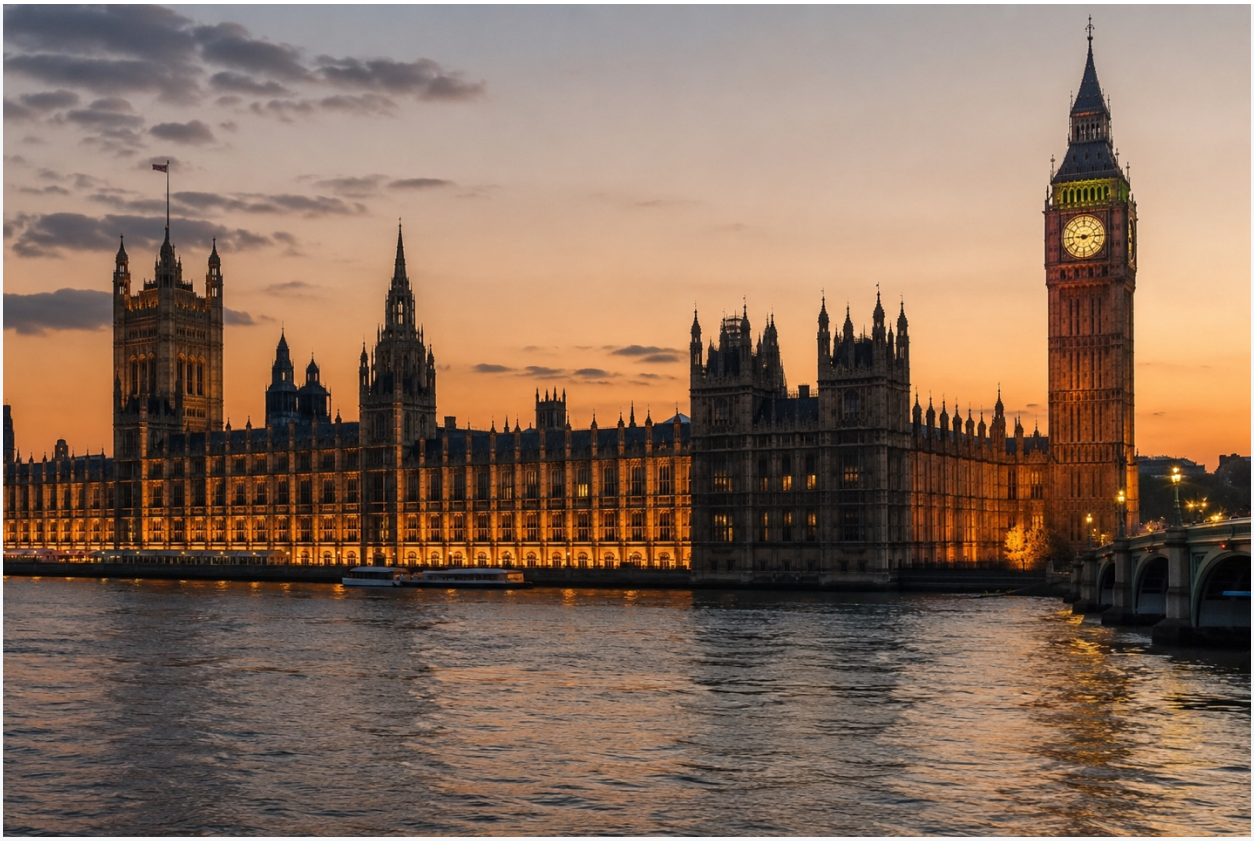
The Cyber Security and Resilience Bill Redraws Who Counts as Critical Infrastructure

The Cyber Security and Resilience (Network and Information Systems) Bill cleared Report Stage and Third Reading in the House of Commons on 16 June 2026. It now moves to the House of Lords. Introduced in November 2025, the Bill updates the NIS Regulations 2018, the framework that has governed cyber security duties for UK critical infrastructure since the EU's NIS Directive was transposed into domestic law. For energy and water utilities, already regulated under that framework, the headline change runs through their suppliers rather than through any new duty on the utility itself.

The Cyber Security and Resilience (Network and Information Systems) Bill cleared Report Stage and moves from the Commons to the Lords.



.

Who's newly in scope

The Bill expands the perimeter of regulated entities in four directions. Data centres above a defined size threshold become Operators of Essential Services for the first time, alongside managed service providers, who have never previously sat inside NIS. Large load controllers, organisations managing large volumes of aggregated smart appliance capacity covering EV chargers, heat pumps and domestic batteries, are brought in directly because of their relevance to energy demand management. And critical suppliers enter the regime not because of which sector they sit in, but because of what would happen if their systems were compromised: a definition built around consequence rather than category.

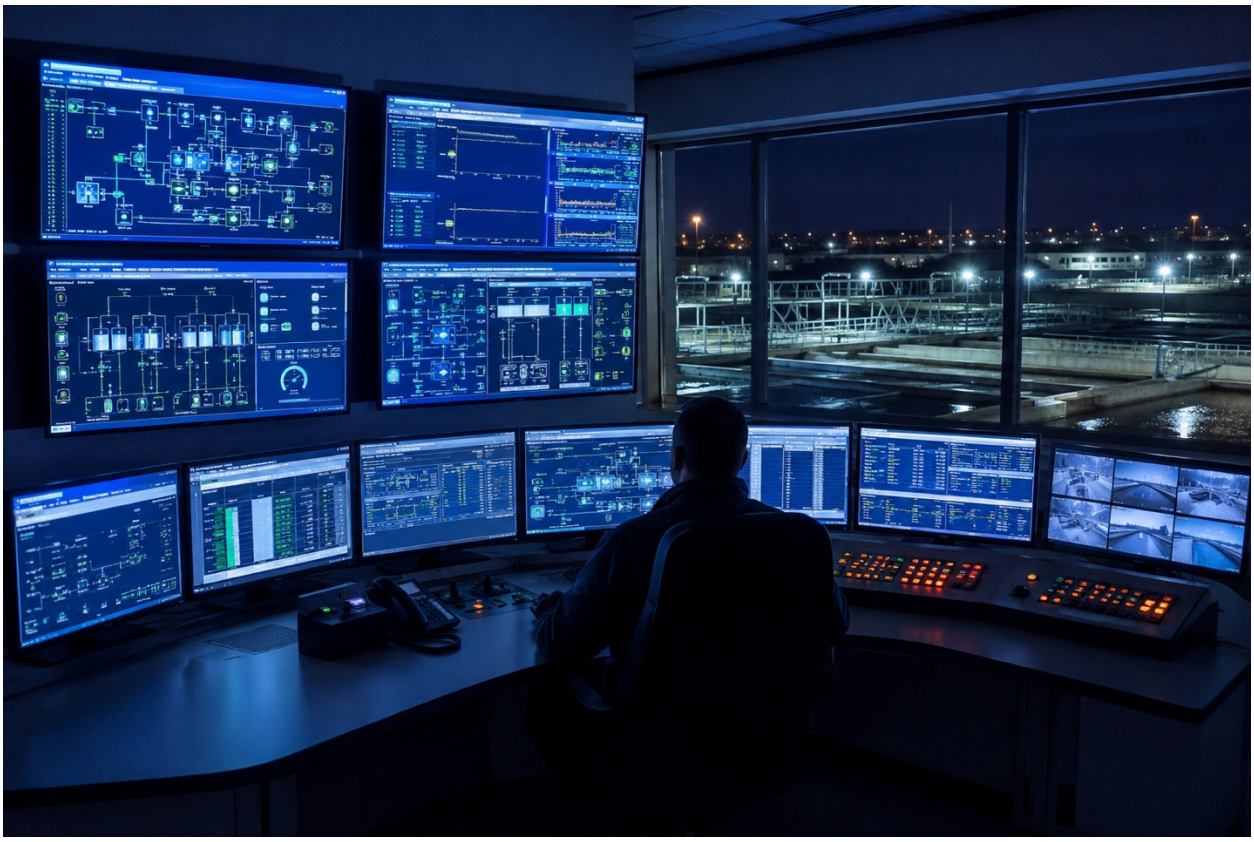
This is not new ground for energy and water

Energy and water companies have carried NIS obligations since 2018, covering electricity, oil and gas, and drinking water as Operators of Essential Services. Ofgem already runs a Cyber Assessment Framework-based assurance regime for downstream gas and electricity OES, with full implementation of its current assurance reporting requirements due for July 2026. The joint DESNZ, NCSC, Ofgem and NESO cyber security strategy published this year sets out board-level expectations for the sector through to 2030, against a backdrop of state-sponsored actors pre-positioning in critical national infrastructure networks.

What changes for utilities is upstream. Critical suppliers carry specific duties under the Bill for the first time. A water or energy company's compliance posture has always depended in part on vendors it does not directly control; now those vendors face their own statutory duties, and the compliance conversation runs in both directions along the contract.

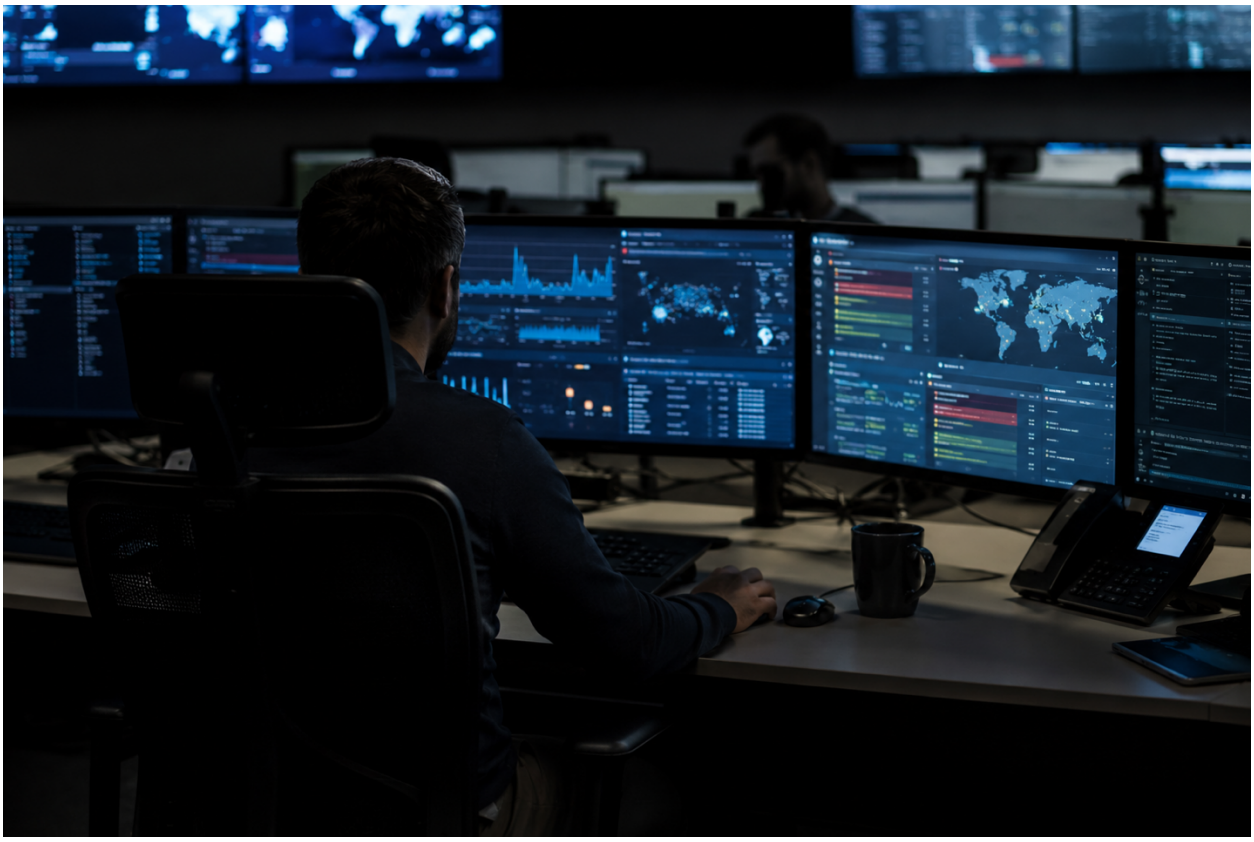
How the supply chain duty bites in practice

Reporting requirements tighten under the Bill: a 24-hour notification to the regulator and the NCSC, followed by a full technical report within 72 hours, applying to both IT and operational technology environments. That OT inclusion matters specifically for utilities running legacy SCADA and ICS infrastructure that was never designed with a 24-hour reporting clock in mind.



The Bill leans on NCSC's Cyber Assessment Framework as its assessment mechanism. CAF v4.0 is structured around four objectives that map closely onto the prevent-detect-respond-recover lifecycle: managing security risk, including asset management (knowing what systems exist on the network) and supply chain oversight; protecting against attack; detecting cyber security events through security monitoring and threat hunting; and minimising the impact of incidents through response and recovery planning. NCSC's own CAF documentation names supply chain oversight as a common gap specifically in OT and ICS environments in energy and water.

The gap is measurable. SANS's 2024 State of ICS/OT Cybersecurity Survey found that 56% of organisations have a dedicated ICS/OT incident response plan; 28% have none at all. Network visibility and monitoring sit among SANS's five critical controls for exactly this reason. Without them, a 24-hour notification deadline depends on someone noticing the incident in time, and manual review is not built for that clock. The CISA/NCSC/FBI quick reference on OT cyber security principles puts the point plainly: incidents cannot be prevented, detected, responded to or recovered from without trained people and the tools to support them.



For newly in-scope managed service providers and critical suppliers, many of whom have not previously had to demonstrate this kind of capability, building OT-aware detection from a standing start, against a live reporting deadline, is a materially different undertaking than adding a clause to an IT security policy.

The number that should move this up the board agenda

The penalties attached to non-compliance are not nominal. Standard breaches carry a maximum penalty of £10 million or 2% of worldwide turnover for an undertaking. More serious breaches rise to £17 million or 4% of turnover. Failure to comply with a national security direction can reach the greater of £17 million or 10% of worldwide turnover, and regulators can impose daily fines of up to £100,000 for continuing contraventions. These figures apply to the newly regulated entities directly, which means a utility's supplier now carries its own direct exposure, not just a contractual obligation passed down from the client.

What to do before Royal Assent, not after

The Bill's scope is still debated. Marks & Spencer and Jaguar Land Rover, both hit by damaging cyber attacks in 2025, sit outside the regulated sectors entirely. The Commons Library briefing flags this gap directly, alongside calls from parts of industry for a single cyber security regulator rather than the current sector-by-sector model. The government has defended the sectoral approach on the basis that different sectors face different risks. Whichever way that debate resolves, it does not change what energy and water CISOs should be doing now.

Two actions do not require Royal Assent first. Review supplier contracts against the Bill's critical supplier duties and NCSC's twelve supply chain security principles, checking whether existing agreements would

survive scrutiny under the new regime. And run an OT asset inventory and incident detection capability assessment before the government's 2026 implementation consultation closes, not as a compliance exercise, but because the 24-hour clock will not wait for either company readiness or final legislative text.

Sources

1. Cyber Security and Resilience (Network and Information Systems) Bill 2026 — Bill text, Report Stage, 27 May 2026
https://bills.parliament.uk/bills/4035

2. Cyber Security and Resilience (NIS) Bill — Summary of the Bill / Summary Factsheet (DSIT, March 2026)
https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill

3. Ofgem NIS Security Assurance Guidance for Downstream Gas and Electricity, 2025
https://www.ofgem.gov.uk/sites/default/files/2025-07/Ofgem-NIS-Security-Assurance-Guidance-Concept-for-DGE-Sector.pdf

4. UK Energy Sector Cyber Security Strategy (2026), joint DESNZ/NCSC/Ofgem/NESO
https://www.gov.uk/government/publications/energy-sector-cyber-security-strategy/energy-sector-cyber-security-strategy

5. NCSC Supply Chain Security: 12 Principles
https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-security-12-principles-infographic

6. Cyber Security and Resilience (Network and Information Systems) Bill 2024-26 — House of Commons Library briefing CBP-10442
https://commonslibrary.parliament.uk/research-briefings/cbp-10442/

7. Cyber Security and Resilience Bill progresses through Parliament — Macfarlanes
https://www.macfarlanes.com/insights/102mlmn/cyber-security-and-resilience-bill-progresses-through-parliament/

8. NCSC Cyber Assessment Framework v4.0
https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf

9. CISA/NCSC/FBI Principles of Operational Technology Cyber Security — quick reference guide, 2024
https://www.cisa.gov/resources-tools/resources/principles-operational-technology-cyber-security

10. SANS 2024 State of ICS/OT Cybersecurity Survey
https://www.sans.edu/cyber-research/sans-2024-state-ics-ot-cybersecurity

11. House of Lords Hansard, 16 June 2026 — Artificial Intelligence: National Security Implications (confirms Commons Report Stage/Third Reading completed same day)
https://hansard.parliament.uk/Lords/2026-06-16/debates/8DB2F2D7-B6BD-4418-89B1-DECF1E4C6F0F/ArtificialIntelligenceNationalSecurityImplications